Sicherheitslecks haben System

Wer IT-Schwachstellen in Unternehmensnetzen analysiert, wird auf Gesetzmäßigkeiten stoßen. Firmen können diese Erkenntnisse nutzen, um Sicherheitslücken zu schließen.

VON GERHARD ESCHELBECK*

Tagtäglich entdecken Experten neue Schwachstellen in Netzen und Anwendungen. Beim Bekanntwerden dieser Lecks stellen sich Administratoren immer wieder die gleichen Fragen: Wie gravierend ist die Schwachstelle? Wie weit ist sie verbreitet? Wie leicht lässt sie sich ausnutzen? Ist irgendeines meiner Systeme von dieser Schwachstelle betroffen?

Die neue Generation automatisierter Viren und Würmer hat den Sicherheitsverantwortlichen gezeigt, dass es nicht ausreicht, sich beim Schutz der Systeme allein auf menschliches Handeln zu verlassen. Jedem zerstörerischen Angriff der letzten Zeit waren Warnungen vor den entsprechenden Schwachstellen vorausgegangen – Wochen, manchmal sogar Monate, bevor die eigentliche Attacke erfolgte. Und trotzdem gelang es den Angreifern, Hunderttausende von PCs und Servern zu treffen.

Hier lesen Sie ...

- welche Gesetzmäßigkeiten sich bei der Analyse von Schwachstellen erkennen lassen;
- wie Unternehmen diese Erkenntnisse nutzen können, um die Gefährdung ihrer IT realistisch zu bewerten;
- wie Best Practices aussehen, die Unternehmen beim Erkennen, Beseitigen und Überprüfen von Sicherheitslücken unterstützen.

Um Schwachstellen in Netzen erfolgreich bekämpfen zu können, müssen Anwender genau verstehen, welche Art von Risiko diese darstellen. Hierbei können Ergebnisse hilfreich sein, die die Analyse von insgesamt sechs Millionen Netzschwachstellen über einen Zeitraum von drei Jahren hinweg erbrachte. Dabei handelt es sich um eine statistisch signifikante, anonymisierte Stichprobe, gezogen aus mehr als 14 Millionen Scans, die global agierende Unternehmen und beliebige Internet-Nutzer vorgenommen hatten, um die Sicherheit ihrer Netzgrenzen und Intranets zu überprüfen. Die zentrale Datenbank umfasst Signaturen für mehr als 4000 verschiedene Sicherheitslücken, die nach CVE, CERT, SANS20 und anderen Quellen standardisiert sind.

Sämtliche Schwachstellendaten sind rein statistischer Natur und können mit keinem Nutzer, System, Unternehmen oder Ort in Verbindung gebracht werden. Bei der Analyse wurden das „Fenster der Gefährdung", die Lebensdauer kritischer Sicherheitslücken, die getroffenen Abhilfemaßnahmen, längerfristige Trends und die Verbreitung von Schwachstellen ermittelt. Dabei ließen sich aufschlussreiche Gesetzmäßigkeiten im Hinblick auf die Halbwertszeit, den Verbreitungsgrad, die Wirkungsdauer und die Ausnutzung feststellen.

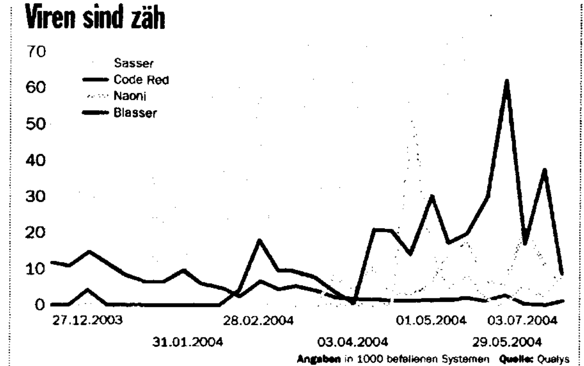
Befall nach Erstinfektion

Die Halbwertszeit einer Schwachstelle ist die Zeit, die vergeht, bis Unternehmen die Hälfte der betroffenen Systeme geschützt haben. Die Halbwertszeit kritischer Schwachstellen beträgt bei externen Systemen 21 Tage und bei internen Systemen 62 Tage; mit abnehmendem Schweregrad verdoppeln sich diese Zahlen. Mit anderen Worten: Selbst bei den gefährlichsten Sicherheitslücken haben Unternehmen nach 21 Tagen erst die Hälfte der anfälligen externen Systeme gepatcht; für die Hälfte der anfälligen internen Systeme benötigen sie 62 Tage. Die restlichen Systeme bleiben somit über einen beträchtlichen Zeitraum hinweg ungeschützt.

Im vergangenen Jahr verkürzte sich die Halbwertszeit von Schwachstellen in Systemen, die direkt an das Internet angebunden sind, von 30 auf 21 Tage – also um 30 Prozent. Das ist eine viel versprechende Entwicklung, die demonstriert, dass die Abwehrmaßnahmen gegen externe Sicherheitslücken besser werden. Andererseits jedoch zeigten Analysen von Schwachstellen innerhalb der Unternehmens-Firewalls, dass diese mit 62 Tagen eine fast 200 Prozent längere Halbwertszeit haben.

Die neuesten Würmer und automatisierten Angriffe nutzten genau dieses Gefahrenfenster aus und richteten sich gegen interne Netze. Über lange Zeiträume hinweg bestehende Angriffsmöglichkeiten in lokalen Netzen stellen somit eine gravierende Schwäche dar. Gezielte Abwehrmaßnahmen sind erforderlich, um diese Risiken zu bewerten und zu vermindern.

Viren sind zäh



Schädlinge wie Sasser, Code Red, Nachi und Blaster verschwinden nie ganz, sondern sorgten beispielsweise im Jahr 2004 immer wieder für Neuinfektionen.

Am Grad der Verbreitung lässt sich das Gefahrenpotenzial einer spezifischen Schwachstelle ablesen, dieser Wert ist einer der Indikatoren für das Auftreten von ausgedehnten – im Gegensatz zu begrenzten – Angriffen. Aufgrund spezieller Bedrohungsprofile unterscheiden sich die meistverbreiteten und kritischsten Schwachstellen in internen Netzwerken von denjenigen, die externe Netze bedrohen. Jedes Jahr treten an die Stelle der kritischsten und am meisten verbreiteten Sicherheitslücken neue Gefahren. Aus diesem Grund sollten die Sicherheitsteams in Unternehmen ihre Abhilfemaßnahmen nach dem Wert der vorhandenen IT-Güter und der Verbreitung der Verwundbarkeiten priorisieren.

Die Abwehr richtet sich nach dem Wert der IT-Güter.

Die Daten zeigen, dass kritische Schwachstellen und ihre Varianten in einer vorhersehbaren Weise wiederkehren und somit eine anhaltende Bedrohung für interne und externe Netze darstellen. Die Schuld daran tragen Anwender großenteils selbst: Neuinfektionen werden häufig durch die Installation neuer Systeme und Server verursacht, auf die Images von fehlerhafter, ungepatchter System- und/oder Anwendungssoftware aufgespielt werden.

Ein entscheidender Faktor für die Stoßkraft einer automatisierten IT-Attacke ist die Zeit: Je schneller Exploit-Code für eine bestimmte Sicherheitslücke geschrieben und in Umlauf gebracht werden kann, desto gefährlicher ist er. Die jüngsten automatisierten Angriffe ließen die „Time-to-Exploit" von Monaten auf Tage schrumpfen und erfolgten damit schneller als jede menschenmögliche Gegenreaktion. Der Analyse zufolge zielen 80 Prozent aller Würmer und automatisierten Angriffe auf die ersten beiden Halbwertszeiten kritischer Schwachstellen. Durch die schnelle Entwicklung von Exploits entstehen in Unternehmen lange Anfälligkeitszeiträume bis zur Sicherung der kritischen Systeme. „SQL Slammer" trat sechs Monate nach der Entdeckung einer Schwachstelle auf, „Nimda" vier Monate und „Slapper" sechs Wochen danach; „Blaster" erschien nur drei Wochen, nachdem ein Sicherheitsleck bekannt geworden war, und der Wurm „Witty" schlug bereits am Tag nach der Veröffentlichung der entsprechenden Sicherheitslücke zu.

Am 19. März 2004 befiel dieser Schädling rund 12 000 Rechner, auf denen Firewalls der Firma Internet Security Systems liefen. Witty erreichte seinen Gipfelpunkt nach zirka 45 Minuten: Zu diesem Zeitpunkt hatte er bereits die meisten anfälligen Hosts infiziert. Laut einer Analyse der Cooperative Association for Internet Data Analysis (CAIDA) und der University of California, San Diego (UCSD), war Witty gleich in mehrerer Hinsicht ein Novum: Er war der erste weit verbreitete Internet-Wurm, der eine zerstörerische Nutzlast trug; er verbreitete sich auf organisierte Weise mit mehr „Ground-Zero-Hosts" als je zuvor; er steht für das bislang kürzeste Intervall zwischen der Bekanntgabe einer Sicherheitslücke und der Freisetzung eines Wurms (ein Tag); er griff nur Hosts an, auf denen eine Sicherheitssoftware lief; und er bewies, dass Anwendungen in einem Nischenmarkt genauso anfällig sind wie die Produkte eines Softwaremonopolisten.

Best Practices zum Schutz

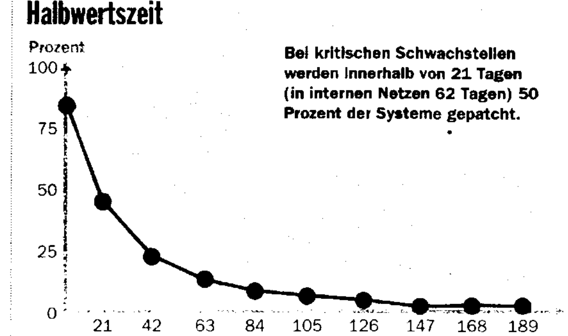
Das Schwachstellen-Management umfasst die Identifizierung, Priorisierung und Behebung von Sicherheitslücken. Getreu dem Motto „Was man nicht messen kann, kann man auch nicht meistern" haben mittlerweile viele Unternehmen erfolgreich ein systematisches Schwachstellen-Management implementiert. Von den Trends, die in den „Gesetzen der Schwachstellen" aufgezeigt werden, lassen sich folgende Best Practices für das Schwachstellen-Management ableiten.

Klassifizierung: Unternehmen sollten sämtliche IT-Ressourcen identifizieren und kategorisieren. Dabei empfiehlt es sich, den jeweiligen Systemen abhängig von ihrer geschäftlichen Bedeutung unterschiedliche Prioritätsstufen zuzuweisen. Kritische Assets sollten alle fünf bis zehn Tage überprüft werden, damit Schwachstellen rechtzeitig ermittelt und Schutzmaßnahmen gegen Exploits getroffen werden können. Assets der unteren Kategorien können, entsprechend ihrer hierarchischen Priorität, weniger häufig gescannt werden, da man hier auch Patches in etwas größeren Zeitabständen einspielen wird.

Kritische Assets alle fünf bis zehn Tage überprüfen.

Priorisierung: Unternehmen sollten ihre Abhilfemaßnahmen anhand der Asset-Klassifikation und der Schwere der Sicherheitslücken priorisieren. Mit dem vor kurzem vorgestellten Common Vulnerability Scoring

Halbwertszeit



Bei kritischen Schwachstellen werden innerhalb von 21 Tagen (in internen Netzen 62 Tagen) 50 Prozent der Systeme gepatcht.

Quelle: Qualys

System (CVSS) steht ein wirkungsvolles Instrument zur Verfügung, um Schwachstellen in einer Unternehmensumgebung die richtige Priorität zuzuweisen.

Integration: Um die Wirksamkeit verschiedener Sicherheitstechnologien wie Server- und Desktop-Erkennungssysteme, Patch-Management-Systeme und Upgrade-Dienste zu verbessern, muss deren Integration mit Schwachstellen-Management-Technologien gewährleistet sein. Außerdem sollte in einem Best-Practice-Unternehmen über die Fortschritte Bericht erstattet werden, die im Hinblick auf die gesteckten Ziele im Bereich Schwachstellen-Management gemacht werden, um so das Bewusstsein für die Sicherheitsproblematik in der Führungsetage zu erhöhen.

Messung: Unternehmen müssen ihre Netze anhand der Halbwertszeitskurve und Wirkungsdauerkurve von Schwachstellen bewerten. Mittels grafischer Darstellungen ist zu verfolgen, wie hoch der Prozentsatz von Schwachstellen ist, der jeweils innerhalb eines 30-tägigen Zyklus beseitigt werden kann, und wie viele Schwachstellen länger als 180 Tage bestehen bleiben. Übersichten über die Leistung des Security-Teams sollten erstellt werden, um zu gewährleisten, dass dessen Arbeit im Endergebnis tatsächlich zu einer Risikominderung führt, insbesondere bei den kritischen Ressourcen.

Audit: Sicherheitsverantwortliche sollten die Resultate der Schwachstellen-Scans nutzen, um festzustellen, wie ihr Unternehmen in puncto Sicherheit insgesamt abschneidet. Mit Hilfe solcher Metriken lässt sich der Erfolg (oder Misserfolg) unterschiedlicher Security-Policies bewerten, um so die Sicherheit zu verbessern. Auch sollten die Ergebnisse genutzt werden, um die Unternehmensleitung über den Sicherheitsstatus zu informieren. *(ave)*

Fazit

Angriffe auf Netze werden immer zahlreicher und raffinierter. Die „Gesetze der Schwachstellen" zeigen **vier Arten von Risiken** für interne und externe Netzwerke auf. Die rechtzeitige und umfassende Erkennung von Sicherheitslücken mit Hilfe **automatisierter Techniken** und die priorisierte Anwendung von Gegenmaßnahmen sind ein wirksames **vorbeugendes Mittel**, mit dem Netz-Manager automatisierte Angriffe abwehren und die Netzsicherheit gewährleisten können.

***GERHARD ESCHELBECK** ist Chief Technology Officer und Vice President of Engineering bei Qualys in Redwood Shores.